Trustwave Secure Web Gateway Security Target

Version 1.5

September 18, 2013

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602
http://www.trustwave.com

REVISION HISTORY

Rev	Description
1.0	November 7, 2012, Initial release
1.1	January 17, 2013, Updates for FSP consistency
1.2	February 20, 2013, Addressed certifier comments
1.3	March 6, 2013, Addressed evaluator comments
1.4	June 6, 2013, Additional changes for TOE boundary and TOE version
1.5	September 18, 2013, Updated the list of documents included in the TOE boundary

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CA ..... Certificate Authority
CC ..... Common Criteria
DBMS ..... DataBase Management System
DLP ..... Data Loss Prevention
EAL ..... Evaluation Assurance Level
GUI ..... Graphical User Interface
HTTP ..... HyperText Transfer Protocol
ICAP ..... Internet Content Adaptation Protocol
IDS ..... Intrusion Detection System
IP ..... Internet Protocol
IT ..... Information Technology
I&A ..... Identification & Authentication
LDAP ..... Lightweight Directory Access Protocol
MSC ..... Mobile Security Client
NTLM ..... NT LAN Manager
SFR ..... Security Functional Requirement
SNMP ..... Simple Network Management Protocol
ST ..... Security Target
SWG ..... Secure Web Gateway
TOE ..... Target of Evaluation
TSF ..... TOE Security Function
URL ..... Uniform Resource Locator

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Trustwave Secure Web Gateway. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Trustwave Secure Web Gateway Security Target, Version 1.5, dated September 18, 2013

1.2 TOE Reference

Trustwave Secure Web Gateway Version 11.0 (Build 18) with Hot Fixes MHF02 and RHF02.

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

1.4 Keywords

Web gateway, threats, risk, collection, analysis.

1.5 TOE Overview

1.5.1 Usage and Major Security Features

Trustwave Secure Web Gateway (SWG) protects against next-generation threats from web site access in real time. By detecting new and targeted attacks, it enables users to access the Internet safely. SWG protects against dynamic, cross-component malware threats using patented real-time code analysis, analyzing the whole composition of a web page.

SWG Real-Time Code Analysis technology provides functionality to detect and block dynamic malware. SWG offers patented technology that instantly analyzes the "intent" of the code and doesn't simply reply on a simple comparison to a list of known, infected sites. As inbound and outbound web communication occurs it is dynamically analyzed and viewed by multiple malware engines to determine intent. These engines run in parallel providing the following abilities:

- Detection and blocking of dynamic malware from cross-component attacks
- Detection of malicious code on web pages
- Comprehensive Web page analysis of both single and multiple component attacks

SWG provides Data Loss Prevention (DLP) functionality by scanning inbound and outbound communication to identify data-stealing malware, including keystroke loggers, phishing attacks, Trojans and root kits. Furthermore, it enforces rules to prevent users from posting or uploading sensitive data.

Policies may be configured to determine the action taken for each web transaction received. The Policies reference Rules that contain Conditions describing the results of the analysis of each transaction. Possible actions are to allow, block, or coach (send an HTTP message to the originator of the transaction to confirm the operation).

SWG may be deployed in an enterprise network in an out of band or in band configuration. Out of band is the typical deployment. In band requires additional hardware (a bypass NIC) and is not supported with virtual appliance distributions; therefore, in band is not included in the evaluation.

Management capabilities are provided via the Management Console, an interactive web-based GUI that supports administrator and user roles. Management Console allows administrators to set policies in the system and assign them to web users or web user groups. Within a given policy, single users or groups of users can be defined as exceptions to the main policy. This ability streamlines the flow of defining users and corresponding rules, and eliminates the need to duplicate policies for fine-tuning the application of a rule. The GUI also provides users with the ability to review security events and audit logs.

SWG supports a hybrid deployment that combines SWG Scanning Servers within the enterprise network with SWG Cloud Scanners and Mobile Security Client (MSC) software. Cloud Scanners are a special type of virtualized scanning server configured to support connections only from user computers running the, or specifically defined proxy servers, for example in remote offices. This functionality is not included in the evaluation.

SWG supports caching of web information in order to accelerate performance. This functionality is not included in the evaluation since it is not security-related and requires an additional (optional) license.

The following additional capabilities of SWG are not included in the evaluation:

- Integration with third party antivirus and DLP solutions to extend the SWG capabilities
- Integration with external Internet Content Adaptation Protocol (ICAP) clients and servers
- High availability configurations
- Integration with VUSafe (a separate product) for approved content functionality
- Integration with external Certificate Authorities (CAs) for certificate validation
- Integration with downstream proxy agents for header pre-authentication
- Integration with external LDAP servers for user authentication

1.5.2 TOE Type

IDS System

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of software executing on either a dedicated physical appliance or virtual appliance (two distinct configurations). The TOE includes the entire appliance (physical or virtual). For the physical appliance, the hardware is part of the TOE. For the virtual appliance, the hardware and hypervisor software are provided by the operational environment.

SWG is available as multiple physical appliance models; all models have equivalent security functionality. The only differences involve processing power and storage capacity, which facilitate processing differing amounts of web application traffic. The SWG 7000 is a blade server supporting one or more blades that operate independently. The following appliance choices are supported.

Table 1 - SWG Appliance Specifications

Model / Item	SWG 3000	SWG 5000	SWG 7000
Rack Space	1U	1U	7U
Power Supplies	1	2	4
Gigabit Ethernet Interfaces	2	4	2 per blade
Requests Per Second (RPS) Processed	124	350	208 per blade
Throughput (Mbps)	11 Mbps	36 Mbps	19 Mbps per blade

The virtual appliance distribution (in the form of an OVF file) must be installed on a server that satisfies the following minimum requirements.

Table 2 - SWG Virtual Appliance Server Minimum Requirements

Item	Requirements
Host Software (Hypervisor)	VMWare ESXI version 4.1
CPUs	IBM X3550 M3 2xQuad-Core Intel E5506 2.1 GHz or equivalent
Memory	4GB

Multiple physical Ethernet interfaces are supported on the SWG appliances. A dedicated management interface is used for HTTP communication between remote browser sessions and the Management Console; this interface is the only TOE interface connected to the management network. It is the responsibility of the operational environment to protect the traffic on the management network from disclosure or modification by unauthorized users.

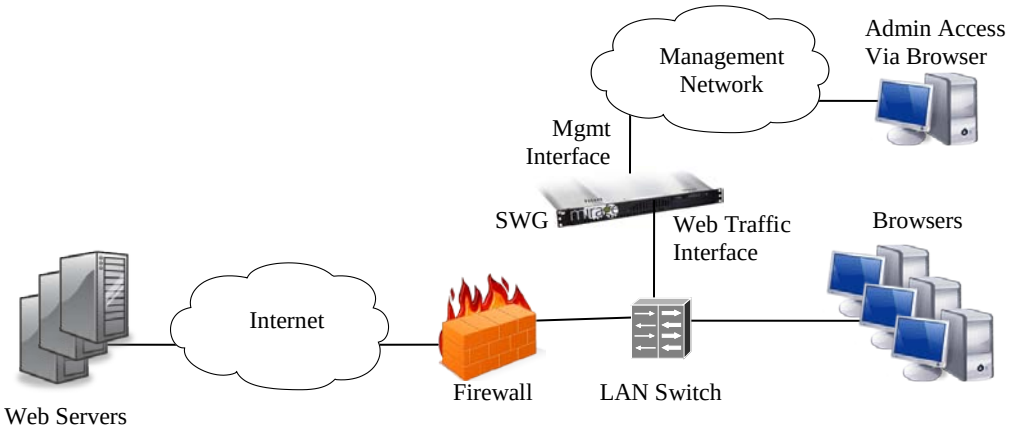
A separate Ethernet interface is used for monitoring the web traffic and responding to security events. This interface is connected to the same network as the web servers.

1.6 TOE Description

The TOE provides functionality to monitor both directions of web traffic, detect security events, and respond to those events according to configured policies.

A typical deployment for the TOE is shown in the following diagram.

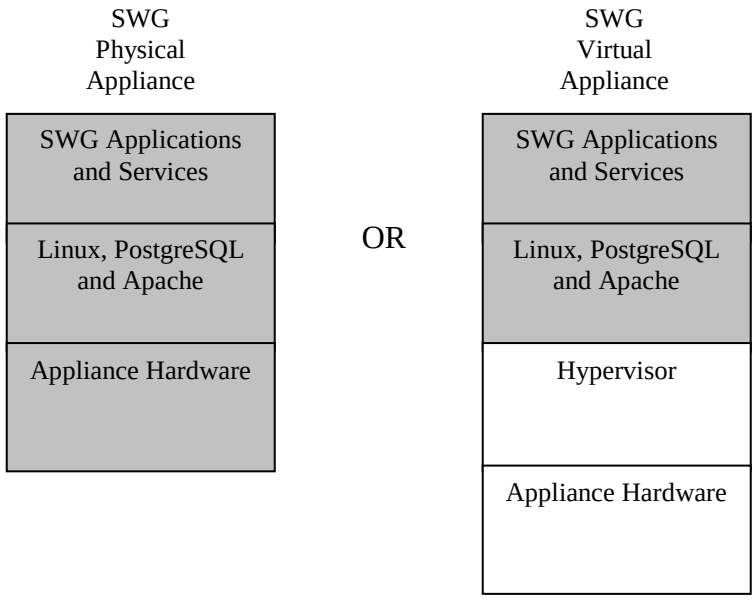
Figure 1 - TOE Deployment



1.6.1 Physical Boundary

The TOE has two distinct configurations – physical appliance or virtual appliance. SWG software is installed on servers with a hardened Linux operating system. The hardened Linux operating system, PostgreSQL DBMS, Apache web server and SWG Software are pre-installed on physical appliances supplied by Trustwave or as a virtual appliance for installation on a qualified server. The physical boundary of the TOE for each configuration is depicted in the following diagram (shaded items are within the TOE boundary).

Figure 2 - Physical Boundary



The physical boundary of the TOE includes the following services and applications distributed by Trustwave to perform the SWG-specific functions described in this document:

1. Web Traffic Monitoring – the main SWG component acts as a service to analyze each received web transaction, apply the applicable Security Policy, and enforce the actions

specified in a matching Rule. This service also saves a copy of web traffic in the Web Log according to the applicable Logging Policy.

2. Management Console – provides a GUI for administrators to control and monitor the operation of the TOE from remote browser sessions. Administrator actions cause audit records to be generated and saved in the
3. Reporting Service – responsible for generating the configured reports according to the specified schedules.

The physical boundary includes the following guidance documentation:

1. *Secure Web Gateway Setup Guide*
2. *Management Console Reference Guide*
3. *Secure Web Gateway Quick Start Guide*
4. *Secure Web Gateway Common Criteria Supplement*

1.6.2 Logical Boundary

1.6.2.1 Audit

Audit records are generated for specific actions performed by users. The audit records are stored on the appliance and may be locally saved on the Console system by authorized administrators of the Console for review outside of the TOE. In the unlikely event audit storage space is exhausted, new audit records are saved (the oldest audit records are deleted).

1.6.2.2 Management

The TOE provides functionality for administrators to configure and monitor the operation of the TOE via the Management Console. Administrator and Super Administrator roles are supported.

The security management functionality provided by the TOE includes:

- Policy management
- Management Console administrator management
- Web user management
- Report management

All TOE data is stored on the appliance.

1.6.2.3 Web Traffic Monitoring

The TOE monitors all web traffic passing through the system. The traffic is analyzed against configured policies to detect security events, and when events are detected the configured reaction is invoked. Users may view the saved information via the Consoles.

Identification Policies may be configured to determine the dynamically determine the identity of the originator sessions against a set of web users defined in the TOE. The identity may be learned by NTLM exchanges with the originating system, examining header fields in the web traffic, or by comparing the originator IP address to information configured for the web users.

The traffic analysis performed by the TOE includes:

- Known signature matching
- Data leakage
- Content file types
- Binary attachment behavior

Logging Policies are also configured to control what web traffic is saved for subsequent review and what information about the traffic is included in the records.

In the unlikely event System data storage space is exhausted, new System data is saved (the oldest System data is deleted).

1.6.2.4 I&A

The TOE identifies and authenticates Management Console users before they are granted access to any TSF functions or data. When valid credentials are presented, security attributes for the administrator are bound to the session.

1.6.3 TOE Data

The following table describes the TOE data.

Table 3 - TOE Data Descriptions

TOE Data	Description
Access Permissions	Specify sets of objects and access permissions that define the access to TSF data by an administrator or administrator group. The object may be a category (e.g. Policies), sub-category (e.g. User Security Policies) or a specific object (e.g. a named User Security Policy). Objects are organized in three containers: M86 for objects that are predefined by the TOE, MyGroup for objects that are created by members of the associated Administrator Group, and Others for objects created by any other Administrator Group. If a permission is not specified for a specific object, the permission for the associated category or sub-category applies. Individual permissions may be set to None, View, Update, or Default (assume the permission of the parent category/sub-category).
Active Content List Condition Component	Specify active content parameters for condition components: • Name • Allowed List • Blocked List
Administrator Groups	Specify parameters for a named administrator group: • Name • Password expiration time • Enforce secure password checkbox • Require password change on first login checkbox • Associated Access Permissions

TOE Data	Description
Administrators	Specify a list of administrator with the following attributes: • Administrator Name • Associated Administrator Group (“Super Administrators” implies the administrator has the Super Administrator role) • Associated Access Permissions (used to override the Administrator Group access permissions) • Email address • Password
Alert Settings	Specify parameters for sending Alerts for each type of system event, including: • Protocol (Email/SNMP) • Email address
Binary Behavior Condition Component	Specify parameters for binary behavior condition components: • Name • Automatic Execution and Termination Authorizations • File Access Authorizations • Registry Authorizations • Network Access Authorizations • Minor Risk Operation Authorizations • Disclosure of Information Authorizations • Java Runtime Authorizations • Change Settings Authorizations • System Settings Authorizations • General Authorizations • Other Running Applications Authorizations
Content Size Condition Component	Specify parameters for content size condition components: • Name • Content Size
Data Leakage Prevention Condition Component	Specify parameters for data leakage prevention condition components: • Name • Filter Conditions
Default Policies	Specify the parameters for the default policies and emergency policy mode for the SWG, including: • Enable Emergency Policy (override all other policies) • Emergency Security Policy • Master Policy • Default Security Policy • Default Logging Policy
Destination Port Range Condition Component	Specify parameters for destination port range condition components: • Name • Port Range
Direction Condition Component	Specify parameters for direction condition components: • Name • Direction (Incoming/Outgoing)
File Extensions Condition Component	Specify parameters for file extensions condition components: • Name • File Extension List

TOE Data	Description
General Parameters	Specify general parameter settings for the SWG operation, including: • Maximum scannable size for files transiting the SWG • Timeouts for client side and server side interactions • Proxy Mode (Explicit or Transparent) • Assigned Policies for Identification, Device Logging, and Upstream Proxy
Header Fields Condition Component	Specify parameters header fields condition components: • Name • Header Fields • Exclude by Headers List
HTTP Method Condition Component	Specify parameters for HTTP method condition components: • Name • Method (GET, POST, LOCK, etc.)
IP Range Condition Component	Specify parameters for IP range condition components: • Name • IP Range
Log Profiles	Specify the filters applied to the log records for display and the information from the records to be included in the display.
Mail Server Settings	Specifies parameters for the mail server used when sending Alerts: • Enable Sending Email checkbox • IP address/hostname • Port • Username • Password • Originating domain
Policy Rule Conditions	Specify parameters for conditions associated with Rules: • Type • Components
Policy Rules	Specify parameters for rules associated with a Policy: • Name • Enable Status • X-Ray Status • Action (Allow/Block/Coach) • Applicable Users (All/Recognized/Unrecognized/explicit) • Excluded Users • Trigger Conditions • End User Block Message • End User Coach Message
Report Definitions	Specify the general parameters for a Report to be generated: • Name • Columns to be included • Filters
Report Schedules	Specify parameters for a schedule for generating a Report from an existing Report Definition: • Name • Associated Report Definition • Schedule • Enable status
Reports	Saved files containing data from a scheduled or saved Report Definition. Reports are accessed via the Management Console.

TOE Data	Description
SNMP Settings	Specifies the parameters used when sending SNMP Traps: • Enable Trap Sending checkbox • Trap port • Destination IP address(es) • SNMP Version • Community
Time Range Condition Component	Specify parameters for time range condition components: • Name • Time Range
True Content Condition Component	Specify parameters for true content condition components: • Name • File Extension List
Upstream Proxy Condition Component	Specify parameters for upstream proxy condition components: • Name • Upstream Proxy List
URL Lists	Specify a list of URLs that can be referenced in URL List Condition Components in Policies.
URL List Condition Component	Specify parameters for URL list condition components: • Name • URL List
User Lists	Specify a list of Users that can be referenced in Policies.
Web User Lists	Specify parameters for a web user list: • Name • List of Assigned Web User Groups and/or Web Users
Web User Policies	Specify the parameters for configured Policies applied to web users for security or logging usage. Parameters include: • Name • Type • Ordered List of Rules • X-Ray Enabled (Security Policies only) • Logging Destinations (Web log, Reports database, and/or Syslog)
Web User Groups	Specify parameters for a named web user group: • Name • List of Associated Users • Assigned Policies • IP Address Range
Web User Identification Policies	Specify the parameters for identification of web users sending traffic through the SWG. Parameters include: • Name • Identification Mechanism (NTLM, Header Fields, Source IP Address)
Web Users	Specify a list of web users with the following attributes: • User Name • Web User Group • Identifiers (IP addresses or USERIDs) • Assigned Policies

1.7 Evaluated Configuration

The evaluated configuration of the TOE includes one instance of SWG executing on a physical or virtual appliance.

The following configuration restrictions apply to the evaluated configuration:

1. Limited Shell Commands are used for installation functions only. Only the management Console is used for control and management of the TOE during operational use.
2. The Master Policy is not assigned to the device or administrators (usage of this functionality is not recommended and is unassigned by default).
3. The system event for disk space exhaustion on the appliance must be configured to send an email and/or SNMP trap.
4. All Administrator accounts are configured to enforce secure passwords, to require password changes upon first login, and to require password changes after a configured period of time.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Common Criteria (CC) for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any Protection profiles.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the Operational Environment.

Table 4 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.MGMTNETWORK	The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

3.3 Threats

The threats identified in the following table are addressed by the TOE and the Operational Environment.

Table 5 - Threats

T.Type	Description
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.Type	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.SCNVUL	Users may take advantage of vulnerabilities in the IT System the TOE monitors to access unauthorized information from the IT system.
T.UNIDENT_ACTIONS	The administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.

3.4 Organisational Security Policies

The Organisational Security Policies identified in the following table are addressed by the TOE and the Operational Environment.

Table 6 - Organisational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ANALYZ	Analytical processes and information to derive conclusions about vulnerabilities must be applied to System data and appropriate response actions taken.
P.DETECT	Events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected and analyzed.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 7 - Security Objectives for the TOE

O.Type	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit and system data information in a human readable form.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The TOE must apply analytical processes and information to the collected information to derive conclusions about vulnerabilities on the IT System it monitors.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.SD_PROTECTION	The TOE will provide the capability to protect system data.
O.TIME	The TOE will provide reliable timestamps.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 8 - Security Objectives of the Operational Environment

OE.Type	Description
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information.

OE.Type	Description
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.INTROP	The TOE is interoperable with the IT System it monitors
OE.MGMTNETWORK	The operational environment will provide a segregated management network interconnecting the TOE components that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.

5. Extended Components Definition

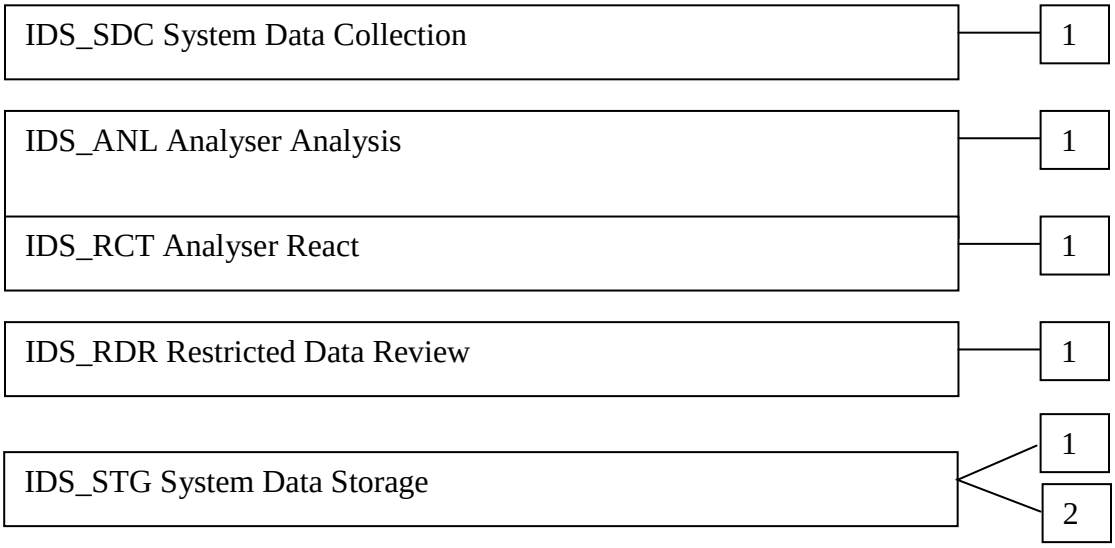
5.1 Extended Security Functional Components

5.1.1 Class IDS: Intrusion Detection

All of the components in this section are based on the class specified in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This class of requirements is taken from the IDS System PP to specifically address the data analysed by an IDS analyzer. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of analyser data and provide for requirements about analyzing, reviewing and managing the data.

Application Note: The PP does not provide hierarchy and dependency information for the extended SFRs defined in the PP. This information has been derived from the model SFRs referenced by the PP.



5.1.1.1 IDS_SDC System Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding collection of information related to security events.

Component Levelling:

IDS_SDC.1 System Data Collection provides for the functionality to require TSF collection of data that may be related to security events.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the events to be collected.

Audit:

There are no auditable events foreseen.

IDS_SDC.1 System Data Collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) **[selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and**

b) **[assignment: *other specifically defined events*].**

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

a) **Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and**

b) **The additional information specified in the Details column of the table below.**

Table 9 - System Data Collection Events and Details

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDs, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDs, location of object, source address, destination address
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Application Note: The rows in this table must be retained that correspond to the selections in IDS_SDC.1.1 when that operation is completed. If additional events are defined in the assignment in IDS_SDC.1.1, then corresponding rows should be added to the table for this element.

5.1.1.2 IDS_ANL Analyser Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of information related to security events.

Component Levelling:

IDS_ANL Analyser Analysis	1

IDS_ANL.1 Analyser Analysis provides for the functionality to require TSF controlled analysis of data collected that is related to security events.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

There are no auditable events foreseen.

IDS_ANL.1 Analyser Analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all System data received:

a) **[selection: *statistical, signature, integrity*]; and**

b) **[assignment: *other analytical functions*].**

Application Note: Statistical analysis involves identifying deviations from normal patterns of behaviour. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a system. For example, patterns of system settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing system settings or user activity at some point in time with those of another point in time to detect differences.

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) **Date and time of the result, type of result, identification of data source; and**

b) **[assignment: *other security relevant information about the result*].**

Application Note: The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.

5.1.1.3 IDS_RCT Analyser React

Family Behaviour:

This family defines the requirements for the TOE regarding reactions to the analysis of information related to security events received from remote IT systems when a vulnerability is detected.

Component Levelling:

IDS_RCT Analyser React	1

IDS_RCT.1 Analyser React provides for the functionality to require TSF controlled reaction to the analysis of data received from remote IT systems regarding information related to security events when an intrusion is detected.

Management:

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

IDS_RCT.1 Analyser React

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_RCT.1.1 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when a vulnerability is detected.

Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The TSF may optionally perform other actions when vulnerabilities are detected; these actions should be defined in the ST.

5.1.1.4 IDS_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the System data collected or generated by the TOE.

Component Levelling:

IDS_RDR Restricted Data Review	1

IDS_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the System data collected or generated by the TOE.

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the System data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read System data that are denied.

b) Detailed: Reading of information from the System data records.

IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

Application Note: This requirement applies to authorised users of the System. The requirement is left open for the writers of the ST to define which authorised users may access what System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

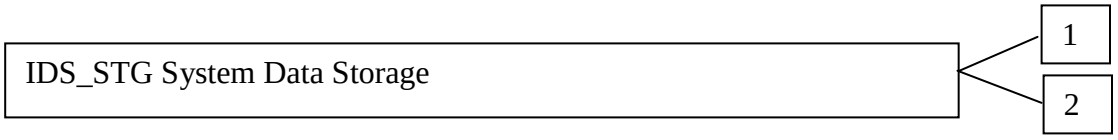
IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

5.1.1.5 IDS_STG System Data Storage

Family Behaviour:

This family defines the requirements for the TOE to be able to create and maintain a secure System data trail.

Component Levelling:



IDS_STG.1 Guarantee of System Data Availability requires that the System data be protected from unauthorised deletion and/or modification and defines the behaviour when specific conditions occur.

IDS_STG.2 Prevention of System Data Loss defines the actions to be taken if the System data storage capacity has been reached.

Management: IDS_STG.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control the System data storage capability.

Management: IDS_STG.2

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of actions to be taken in case System data storage capacity has been reached.

Audit: IDS_STG.1

There are no auditable events foreseen.

Audit: IDS_STG.2

There are no auditable events foreseen.

IDS_STG.1 Guarantee of System Data Availability

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

Application Note: Authorised deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

IDS_ STG.1.3 The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].

Application Note: The ST needs to define the amount of System data that could be lost under the identified scenarios.

IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection
IDS_ANL.1 Analyser Analysis

IDS_STG.2.1 The System shall [selection: *'ignore System data', 'prevent System data, except those taken by the authorised user with special rights', 'overwrite the oldest stored System data'*] and send an alarm if the storage capacity has been reached.

Application Note: The ST must define what actions the System takes if the result log becomes full. Anything that causes the System to stop analysing events may not be the best solution, as this will only affect the System and not the system on which it is analysing data (e.g., shutting down the System).

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the security requirements that are provided by the TOE.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* and/or the previous chapter of this document with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The events in the following table.*

Table 10 - Auditable Events

SFR	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
	Access to System	IP address of the remote system
FIA_UAU.2	Use of the authentication mechanism	User identity, location
FIA_UID.2	Use of the identification mechanism	User identity, location
FMT_MTD.1	Modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the Administrator IP address and SWG IP address*.

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *administrators* with the capability to read *all data* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.4 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that *the most recent* stored audit records will be maintained when the following conditions occur: audit storage exhaustion.

Application Note: In the unlikely event audit storage space is exhausted, new audit records are saved (the oldest audit records are deleted).

6.1.1.5 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and *send an Alert* if the audit trail is full.

Application Note: In the unlikely event audit storage space is exhausted, new audit records are saved (the oldest audit records are deleted).

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *Web Firewall SFP* on

1. *Subjects: Remote systems sending HTTP messages*
2. *Information: HTTP messages and attachments received from remote systems*
3. *Operations: Allow, Block, Coach.*

Application Note: Coach refers to sending an HTTP message to the remote system that sent the HTTP message, asking for confirmation that the HTTP message should be forwarded.

6.1.2.2 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *Web Firewall SFP* based on the following types of subject and information security attributes:

1. *Presumed source address of the remote system sending the HTTP message*
2. *HTTP message contents*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. *The HTTP message contents are analyzed to determine what conditions apply.*
2. *The configured Policies are applied to the HTTP message and conditions to determine if any Rules are satisfied. Rules are checked in the priority order specified in the Policy.*
3. *The action (Allow, Block, Coach) specified in the first Rule that is satisfied is performed.*
4. *If the action is Coach, the MTTP message is temporarily saved while an HTTP message is sent to the originating remote system requesting confirmation that the message that should allowed.*

FDP_IFF.1.3 The TSF shall enforce the *no additional information flow control SFP rules*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

1. *If no Rules are satisfied, the action is implicitly Allow.*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *none*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) *Administrator name;*
b) *Password;*
c) *Associated Administrator Group;*
d) *Email address;*
e) *Permissions.*

6.1.3.2 FIA_UAU.2 User Authentication Before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *create* the *data identified in the following table* to *the authorised identified roles identified in the following table.*

Application Note: For each object, the access permission for it may be configured as "None", "View" or "Update".

Table 11 - TSF Data Access Details

TSF Data	Super Administrator	Administrator with "None"	Administrator with "View"	Administrator with "Update"
Access Permissions	Query and Modify	n/a	n/a	n/a
Condition Component	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Administrator Groups	Create, Query, Modify and Delete	n/a	n/a	n/a
Administrators	Create, Query, Modify and Delete	n/a	n/a	n/a
Alert Settings	Query and Modify	n/a	n/a	n/a
Default Policies	Query	None	Query	Query
General Parameters	Query and Modify	n/a	n/a	n/a
Log Profiles	Create, Query, Modify and Delete their own profiles	Create, Query, Modify and Delete their own profiles	Create, Query, Modify and Delete their own profiles	Create, Query, Modify and Delete their own profiles
Mail Server Settings	Query and Modify	n/a	n/a	n/a
Policy Rule Conditions	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Policy Rules	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Report Definitions	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Report Schedules	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Reports	Create, Query, and Delete	None	Query	Create, Query, Modify and Delete
SNMP Settings	Query and Modify	n/a	n/a	n/a
URL Lists	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete

TSF Data	Super Administrator	Administrator with "None"	Administrator with "View"	Administrator with "Update"
User Lists	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Web User Lists	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Web User Policies	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Web User Groups	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Web User Identification Policies	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete
Web Users	Create, Query, Modify and Delete	None	Query	Create, Query, Modify and Delete

6.1.4.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) Web user management;

b) Policy management;

c) Administrator management;

d) Log Profile management;

e) Report management.

6.1.4.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Administrator and Super Administrator.*

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time-stamps.

6.1.6 Intrusion Detection (IDS)

6.1.6.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) network traffic,; and

b) *no other events*.

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the Details column of the table below.

Table 12 - System Data Collection Events and Details

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

6.1.6.2 IDS_ANL.1 Analyser Analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all System data received:

a) signature and

b) *content behavior, content type, and data leakage*.

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) *associated HTTP message*.

6.1.6.3 IDS_RCT.1 Analyser React

IDS_RCT.1.1 The System shall send an alarm to *the configured Syslog server for Logging Policies* and take *the configured Security Policy actions* when a vulnerability is detected.

6.1.6.4 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The System shall provide *authorised administrators* with the capability to read *Web Log records and Reports* from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.1.6.5 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

IDS_ STG.1.3 The System shall ensure that *new* System data will be maintained when the following conditions occur: System data storage exhaustion.

6.1.6.6 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall overwrite the oldest stored System data and send an alarm if the storage capacity has been reached.

6.2 TOE Security Assurance Requirements

The assurance requirements are identified in the following table. These requirements reference Part 3 of the *Common Criteria for Information Technology Security Evaluation*.

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 13 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 14 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied by FAU_STG.2
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied

SFR	Hierarchical To	Dependency	Rationale
FDP_IFF.1	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied Not satisfied. See note below.
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
FPT_STM.1	No other components.	None	na
IDS_SDC.1	No other components.	FPT_STM.1	Satisfied
IDS_ANL.1	No other components.	IDS_SDC.1	n/a
IDS_RCT.1	No other components.	IDS_ANL.1	Satisfied
IDS_RDR.1	No other components.	IDS_SDC.1 IDS_ANL.1	Satisfied Satisfied
IDS_STG.1	No other components.	IDS_SDC.1 IDS_ANL.1	Satisfied Satisfied
IDS_STG.2	No other components.	IDS_SDC.1 IDS_ANL.1	Satisfied Satisfied

Note regarding FMT_MSA.3: FDP_IFF.1 specifies the following security attributes: the presumed IP address of the remote system, and the HTTP message contents. These attributes are dynamically extracted from each HTTP message received. Since they are never configured by an administrator, FMT_MSA.3 is not required.

7. TOE Summary Specification

7.1 FAU_GEN.1, FPT_STM.1 [Audit]

The TOE generates audits for the events specified in the table included with FAU_GEN.1(1). Startup and shutdown of the audit function is equivalent to startup and shutdown of the SWG software components; these audit records are stored in the System Log. The following fields are included in all audit log records, although not all fields are populated in all records:

- Date/time
- SWG IP address
- Message (details of the event)
- Severity (Error or Normal)

Audit records for actions taken by Administrators are stored in the Audit Log. The following fields are included in all audit log records, although not all fields are populated in all records:

- Administrator name (user identity)
- Date/time (the TOE maintains reliable timestamps)
- Administrator IP address (location)
- SWG IP address
- Message (details of the Administrator action)

The audits records are maintained by the TOE in the database on the appliance in plain text.

7.2 FAU_SAR.1, FAU_SAR.2 [Audit]

Audit records may be viewed via the Management Console by any authorized Administrator using Log View or Reports.

7.3 FAU_STG.2, FAU_STG.4 [Audit]

The user access functionality of the TOE does not provide any mechanism to modify or delete audit records. If no space is available in the database when the TOE attempts to insert a new audit record, the oldest audit records are deleted and the new audit record is saved in the database. When this occurs, an Alert is generated and a message is sent to the Alert destination configured for disk space exhaustion.

7.4 FIA_ATD.1 [Management, I&A]

The TOE maintains the following information for each user account:

- Administrator name;
- Password;
- Assigned Administrator Group;
- Email address;
- Permissions.

User account information is stored in the database on the SWG appliance.

7.5 FIA_UAU.2, FIA_UID.2 [I&A]

The TOE requires all users of the Management Console to successfully identify and authenticate themselves via a username and password before access is granted to any TSF data or functions. Validation of the supplied credentials is performed by the TOE.

7.6 FMT_MTD.1 [Management]

The TOE grants access to TSF data via the Management Console according to the permissions specified in the table included with FMT_MTD.1(1). The Management Console may only be used by authorized administrators. Access to TSF data other than that specified in the table is prevented.

7.7 FMT_SMF.1 [Management]

The TOE provides functionality for authorized users to manage the following items via the Console:

- Web user management;
- Policy management;
- Administrator management;
- Log Profile management;
- Report management.

7.8 FMT_SMR.1 [Management]

All interactive users of the Management Console are required to successfully complete I&A, at which time the permissions configured for the administrator are associated with the user session. The permissions assigned to the user account determine the access permissions for the user per the table with FMT_MTD.1. Administrators assigned to the Super Administrator group are implicitly granted Update access to all TSF data.

7.9 IDS_SDC.1, IDS_ANL.1, IDS_RCT.1, FDP_IFC.1, FDP_IFF.1 [Web Traffic Monitoring]

The TOE receives web traffic. The traffic is used for analysis against configured policies and to determine the action taken for individual transactions.

As network traffic is received, it is analyzed by the TOE. Analysis includes signature detection, detection of data leakage, and determination of attachment file types and behavior of binary content. Attachment file types are analyzed both by examining the claimed file extensions and by actual content. The results of the analysis are saved as Conditions that can be referenced in Rules.

The binary behavior engine is based on checking security behaviors and profiles, which are examined through the inspection of each binary's exposed mechanisms defined as required interfaces to the system. The engine enables active content identification that could be considered malicious or suspicious when exhibited by ActiveX Controls, Java Applets, executable files and any other relevant files.

Rules are contained within multiple types of Policies. In turn, Rules may contain multiple Conditions. Rule processing is performed as follows:

1. Only enabled Rules are processed.
2. For a Rule to be enforced, **all** its Conditions must be matched.
3. Rules are enforced in the order determined by the Rule priority list within the Policy
4. Any action taken is according to the Rule of highest priority matching a given transaction.
5. After a Rule is enforced, lower priority Rules are no longer relevant and are not evaluated.
6. If no Rule matches, an Allow action is implied for the Policy.

If the traffic is for a new session, the Identification Policy is checked to determine the mechanism used to identify the web user associated with the session. Options include using NTLM to obtain the USERID from the IT system that originated the session, extracting the identity from header fields in the transaction and matching that information against the Web Users, or matching the IP address of the IT system that originated the session against the Web Users. If the identity can't be determined, the Policies assigned to the Unrecognized Users Group apply. Otherwise the Policies assigned to the Web User or Web User Group of the Web User apply.

For each HTTP Request or Response analyzed, the applicable User Security Policy is first evaluated. If Emergency Policies are enabled, the applicable User Security Policy is the Emergency Security Policy; otherwise, it is the User Security Policy determined via the Identification Policy.

If HTTPS is used for web site access (rather than HTTP), then the applicable HTTPS Policy also is applied to the traffic analysis. HTTPS Policies define which HTTPS sites are fully allowed, which HTTPS sites are inspected, which HTTPS sites request user approval to continue, and which HTTPS sites are blocked. The blocking mechanism is based on White Lists, URL categorization, certificate error checking, and certificate validation.

The actions for the highest priority Rule that matches in any Policy are performed. Allow actions permit the transaction to be forwarded through the TOE (subject to subsequent analysis) and lower priority Rules within the Policy are not evaluated. If the Policy or Rule is in X-Ray mode, then Block and Coach actions are not performed but the associated logging is performed. When X-Ray mode is not set, then Block and Coach actions are processed as follows:

1. Requests
    a. Block - the request is not sent to the destination server, and the configured end user message is forwarded to the user.
    b. Coach - the configured end user message is forwarded to the user. If the user then approves the message, the request is sent to the destination server.
2. Responses
    a. Block - the content in the response is not passed to the user, and the configured end user message is forwarded to the user.

The applicable Logging Policy determines whether information concerning the traffic is logged to the Web Log, the Reports database, and/or Syslog. The Device Logging Policy determines

whether information concerning identification activity is logged to the Web Log, the Reports database, and/or Syslog. Security events are contained within the records as Conditions. The information for each record that may be included is:

- HTTP transaction
- Transaction content
- Originating IP address
- Web user name
- Date/Time
- Action (Allow/Block/Coach)
- Conditions (analysis results)
- X-Ray mode
- Applicable Security Policy name
- Matched Security Rule name
- Applicable Identification Policy name
- Matched Identification Rule name

7.10 IDS_RDR.1 [Web Traffic Monitoring]

The TOE provides authorized administrators with the ability to read Web Logs (including captured traffic) in a human readable form via the Management Console. The information is presented through Log Views and Reports.

7.11 IDS_STG.1, IDS_STG.2 [Web Traffic Monitoring]

The user access functionality of the TOE does not provide any mechanism to modify System data. System data may be deleted by authorized users. If no space is available in the database when the TOE attempts to insert new System data, the oldest information is deleted and the new information is saved. When this occurs, an Alert is generated and a message is sent to the Alert destination configured for disk space exhaustion.

8. Protection Profile Claims

Conformance to a Protection Profile is not claimed.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each organizational security policy, threat and assumption, the security objective(s) that address it.

Table 15 - Security Objectives Mapping

	O.ACCESS	O.AUDITS	OE.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.SD_PROTECTION	O.TIME	OE.AUDIT_SORT	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.MGMTNETWORK	OE.PERSON	OE.PHYCAL	OE.PROTECT
A.ACCESS																		X				
A.ASCOPE																		X				
A.DYNMIC																		X		X		
A.LOCATE																					X	
A.MANAGE																				X		
A.MGMTNETWORK																			X			
A.NOEVIL																X	X				X	
A.NOTRUST																X					X	
A.PROTCT																					X	
P.ACCACT		X					X							X	X							
P.ACCESS	X		X				X				X		X									
P.ANALYZ						X						X		X								
P.DETECT						X		X						X								
P.INTGTY			X						X				X									
P.MANAGE	X				X		X				X					X	X			X		
P.PROTCT										X											X	X
T.COMDIS	X						X				X											X
T.COMINT	X						X		X		X											X
T.IMPCON	X				X		X										X					
T.LOSSOF	X						X		X		X											
T.MISACT								X														
T.MISUSE								X														
T.PRIVIL	X						X				X											
T.SCNVUL						X		X														
T.UNIDENT_ACTIONS		X		X										X								

The following table describes the rationale for the security objectives mappings.

Table 16 - Rationale For Security Objectives Mappings

Item	Security Objectives Rationale
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.MGMTNETWORK	The OE.MGMTNETWORK objective ensures that the TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRUST	The TOE can only be accessed by authorized users. The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE software and the hardware on which it is installed.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_SORT objective supports this policy by providing a mechanism for administrators to sort the audit logs for effective review.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.AUDIT_PROTECTION and O.SD_PROTECTION objectives counter this threat via TOE protections of the audit trail and System data storage. The O.PROTCT objective addresses this policy by providing TOE self-protection.

Item	Security Objectives Rationale
P.ANALYZ	Analytical processes and information to derive conclusions about vulnerabilities must be applied to System data and appropriate response actions taken. The O.IDANLZ objective requires analytical processes be applied to data collected. The O.RESPON objective requires the TOE to respond appropriately to the detected vulnerabilities. The O.TIME objective supports this policy by providing a time stamp for insertion into the System data records.
P.DETECT	Events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected and analyzed. The O.IDSENS and O.IDANLZ and objectives address this policy by requiring collection and analysis of network traffic for the monitored IT Systems. The O.TIME objective supports this policy by providing a time stamp for insertion into the System data records.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of data from modification. The O.AUDIT_PROTECTION and O.SD_PROTECTION objectives ensure the protection of audit and System data.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions (overflows) of audit and System data storage (these are the only TOE data items that are dynamically created without human interaction). The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures the integrity of all audit and System data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.

Item	Security Objectives Rationale
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE to collect Sensor data.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.IDSENS objective addresses this threat by requiring a TOE to collect Sensor data.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.SCNVUL	Users may take advantage of vulnerabilities in the IT System the TOE monitors to access unauthorized information from the IT system. The O.IDSENS and O.IDANLZ objectives counter this threat by requiring a TOE to collect and analyze traffic involving the IT System to detect indications of a vulnerability.
T.UNIDENT_ACTIONS	The administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach. The O.AUDITS objective helps to mitigate this threat by recording actions for later review. The O.AUDIT_REVIEW objective helps to mitigate this threat by providing the Administrator with the ability to review the actions taken by administrators. The O.TIME helps to mitigate this threat by ensuring that correct timestamps are available for audit records.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 17 - SFRs to Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.EADMIN	O.IDAUTH	O.IDANLZ	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.SD_PROTECTION	O.TIME
FAU_GEN.1		X												
FAU_SAR.1				X										
FAU_SAR.2				X										
FAU_STG.2	X	X	X			X			X	X	X			
FAU_STG.4		X								X				
FDP_IFC.1							X					X		
FDP_IFF.1							X					X		
FIA_ATD.1						X								
FIA_UAU.2	X					X								
FIA_UID.2	X					X								
FMT_MTD.1	X		X			X			X		X		X	
FMT_SMF.1	X				X				X					
FMT_SMR.1			X			X							X	
FPT_STM.1														X
IDS_ANL.1							X							
IDS_RCT.1												X		
IDS_RDR.1	X					X								
IDS_SDC.1								X						
IDS_STG.1	X					X			X	X	X		X	
IDS_STG.2										X				

The following table provides the detail of TOE security objective(s).

Table 18 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. Authorized users are granted access to data based upon their configured security attributes [FMT_MTD.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion [FAU_STG.2, IDS_STG.1]. The appropriate TOE management functions are identified [FMT_SMF.1].

Security Objective	SFR and Rationale
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must prevent unauthorized modification and deletion of audit data as well as the loss of collected data in the event the audit trail is full [FAU_STG.2, FAU_STG.4].
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information. The TOE protects the audit records from unauthorized modification or deletion [FAU_STG.2]. Access privileges to the audit trail is determined by the user role [FMT_SMR.1] and strictly defined [FMT_MTD.1].
O.AUDIT_REVIEW	The TOE will provide the capability to view audit and system data information in a human readable form. Authorized administrators may review the audit records [FAU_SAR.1]. This functionality is only provided to authorized administrators [FAU_SAR.2].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The management functions provided by the TOE are specified [FMT_SMF.1].
O.IDANLZ	The TOE must apply analytical processes and information to the collected information to derive conclusions about vulnerabilities on the IT System it monitors. The Analyzer is required to perform vulnerability analysis and generate conclusions [IDS_ANL.1]. The TOE applies the configured Policies to each HTTP message to determine the appropriate action [FDP_IFC.1, FDP_IFF.1].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. Authorized users are granted access to data based upon their configured security attributes [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [FAU_STG.2, IDS_STG.1].
O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets. The TOE is required to collect events indicative of vulnerabilities on IT System being monitored [IDS_SDC.1].
O.INTEGR	The TOE must ensure the integrity of all audit and System data. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion [FAU_STG.1, IDS_STG.1]. The functions made available to users for management of the TOE are limited [FMT_SMF.1].

Security Objective	SFR and Rationale
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows. The TOE must prevent unauthorized modifications and deletions and the loss of audit data in the event the audit trail is full [FAU_STG.2, FAU_STG.4]. The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [IDS_STG.1].
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The System is required to protect the audit trail and System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [FAU_STG.2, IDS_STG.1].
O.RESPON	The TOE must respond appropriately to analytical conclusions. The TOE is required to respond as configured in the event a vulnerability is detected [IDS_RCT.1]. The TOE applies the configured Policies to each HTTP message to determine the appropriate action [FDP_IFC.1, FDP_IFF.1].
O.SD_PROTECTION	The TOE will provide the capability to protect system data. The TOE protects the system data from unauthorized modification or deletion [IDS_STG.1]. Access privileges to the system data is determined by the user role [FMT_SMR.1] and strictly defined [FMT_MTD.1].
O.TIME	The TOE will provide reliable timestamps. The TOE is required to provide reliable timestamps [FPT_STM.1].

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.2 from part 3 of the Common Criteria.